Claims:

1. An authentication protocol for increasing safety against a man-in-the-middle computer access attack for point-to-point communication, between a client computer and a server, to services in at least one of a network for data and telecommunication utilizing a challenge-response pattern, comprising:

transmitting through a client computer an authentication request containing a clients username to a server providing said services, said server identifying said client computer IP address and a client password accessible by the server through the transmitted username;

said server responding with an N byte nonce numerical value;

said client computer utilizing a hash algorithm to compute a hash value of at least the parameters clients password, client computer unique IP address, server unique IP address, and said nonce value;

transmitting said hash value through said client computer as an authenticator for accessing said services; and

said server reproducing said authenticator by utilizing said hash algorithm and the parameters clients accessible password, client computer unique IP address, server unique IP address, and said nonce value, comparing the reproduction with the transmitted authenticator, and granting an access to said server and services if said reproduced authenticator matches said transmitted, thus by utilizing said client computer unique IP address and said server unique IP address in said authenticator preventing a man-in-the-middle computer, having a different IP address, from addressing said server with a matching authenticator.

2. The protocol according to claim 1, wherein said N byte nonce is a random data only generated once by a random generator and used once in said point-to-point communication and then discarded.

3. The protocol according to claim 2, wherein the random generator is provided a seed to produce said nonce numerical value.

4. The protocol according to claim 3, wherein the seed is comprised of said password and a volatile value.

5. The protocol according to claim 4, wherein the volatile value is a timestamp value or a counter value.

6. The protocol according to claim 1, wherein said parameters are concatenated in an arbitrary order before said hash algorithm is applied.

7. The protocol according to claim 1, wherein said hash algorithm is one of SHA-1, SHA-256, SHA-384 and SHA-512.

8. The protocol according to claim 1, wherein said hash algorithm is an HMAC utilizing said password as a key.

9. The protocol according to claim 1, wherein a salt value is concatenated to said password before it is hashed.

10. An authenticator signal utilized in a protocol for increasing safety against a man-in-the-middle computer access attack for point-to-point communication, between client computer and server, to services in at least one of a network for data and telecommunication, said signal comprising:

the hash value of at least the parameters clients password, client computer unique IP address, server unique IP address, and an N byte nonce value constituting said authenticator signal for accessing said services; and

said authenticator signal comprising said client computer unique IP address and said server unique IP address, thus preventing said authenticator signal from being sent from a computer with a different IP address.

11. The signal according to claim 10, wherein said N byte nonce value is a random data only generated once by a random generator and used once in said point-to-point communication and then discarded.

12. The signal according to claim 11, wherein the random generator is provided a seed to produce said nonce numerical value.

13. The signal according to claim 12, wherein the seed is comprised of said password and a volatile value.

14. The signal according to claim 13, wherein the volatile value is a timestamp value or a counter value.

15. The signal according to claim 10, wherein said parameters are concatenated in an arbitrary order before said hash algorithm is applied.

16. The signal according to claim 10, wherein said hash algorithm is one of SHA-1, SHA-256, SHA-384 and SHA-512.

17. The signal according to claim 10, wherein said hash algorithm is an HMAC utilizing said password as a key.

18. The signal according to claim 10, wherein a salt value is concatenated to said password before it is hashed.

19. A medium for carrying an authenticator signal utilized in a protocol for increasing safety against a man-in-the-middle computer access attack for point-to-point communication, between a client computer and a server, to services, whereby said signal

comprises the hash value of at least the parameters clients password, client computer unique IP address, server unique IP address, and an N byte nonce value constituting said authenticator signal for accessing said services, and said authenticator signal comprising said client computer unique IP address and server unique IP address, thus preventing said authenticator signal from being sent from a computer with a different IP address in said medium, said medium being a network for at least one of data and telecommunication.

20. A detector in a server for increasing safety against a man-in-the-middle computer access attack for point-to-point communication, between a client computer and said server, to services in at least one of a network for data and telecommunication utilizing a challenge-response pattern, comprising:

detection of a transmission, through what is believed to be a client computer, of an authentication request containing a clients username to a server providing said services, said server identifying said client computer IP address and a client password accessible by the server through the transmitted username;

said server responding with an N byte nonce numerical value;

said client computer utilizing a hash algorithm to compute a hash value of at least the parameters clients password, client computer unique IP address, server unique IP address, and said nonce value;

transmitting said hash value through said client computer as an authenticator for accessing said services; and

said server reproducing said authenticator by utilizing said hash algorithm and the parameters clients accessible password, client computer unique IP address, server unique IP address, and said nonce value, comparing the reproduction with the transmitted authenticator,

whereby said detector detects a difference between the reproduction and the transmitted authenticator determining a man-in-the-middle computer attack.

21. A detector according to claim 20, wherein the IP address of the man-in-the-middle computer is determined by reverse analyzing the transmitted authenticator by utilizing the reproduced correct authenticator.